UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,981	07/26/2001	Igor G. Muttik	NAI1P018/01.095.01	8531

28875 7590 02/10/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 02/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/916,981	MUTTIK ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-33 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-33 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 26 July 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 20010904.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1-33 are pending.

Claim Objections

1. Claims 9, 14, 23, 28, 31, 32, and 33 are objected to under 37 CFR 1.75(a) because of the following informalities:

- Claim 9, line 2; claim 14, line 3; claim 23, line 2; claim 28, line 3; claim 31, line 9; claim 32, line 7; and claim 33, line 7 all recite the limitation "the network". There is insufficient antecedent basis for this limitation in the claims. For purposes of prior art rejection, it has been construed as "a network".
- Claim 31, lines 5 and 6: "fingerprints associated with fingerprints of innocent data" should be "fingerprints associated with innocent data".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-7, 9-12, 14-21, 23-26, 28, 29, and 30-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kephart et al. (U.S. Patent 5,613,002) in view of

Wells (U.S. Patent 6,338,141) and Albrecht (U.S. Patent Application Publication 2001 / 0,005,889).

Regarding Claim 1,

Kephart et al. disclose a method for detecting viruses in software, comprising:

Comparing the data with fingerprints of innocent data in a second database (Column 5, lines 2-13); and

Allowing access to the data if the data is successfully compared to the fingerprints of innocent data (Column 5, lines 33-36). It would only take 1 reconstruction to determine that the current file matches that of the fingerprint for that file.

Kephart et al. do not disclose comparing the data with a virus database or transmitting the data to a server.

Wells, however, discloses the steps of comparing data with a plurality of virus definitions in a first database (Column 9, lines 19-20) and executing a security event if the data is successfully compared with at least one of the virus definitions (Column 9, lines 25-26). This new method would be the method of Kephart et al. comparing the data against signatures of known viruses in a virus database.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use this other form of virus detection in order to expand the viruses that are detected by the system. One of

ordinary skill in the art would have been motivated to do so because Kephart et al. suggest the use of other virus scanning software in combination with his method (Kephart et al., Column 12, lines 55-57).

Wells does not disclose transmitting the data to a server.

Albrecht, however, discloses the step of transmitting information to a server for analysis purposes if the client machine cannot identify the data as being either virus or innocent (Detailed Description, Paragraph 47). This new method would be the method of Kephart et al. modified by Wells sending information to a server for further analysis.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to send information to a server for analysis in order to allow for fewer databases to be updated every time there is a new virus. One of ordinary skill in the art would have been motivated to do so in order to reduce the number of virus updates required, improving security of the network (Background, Paragraphs 2 and 3).

Regarding Claim 15,

Claim 15 is a computer program product claim that is substantially equivalent to method claim 1. Therefore, claim 15 is rejected under a similar rationale.

Regarding Claim 29,

Claim 29 is a system claim that is substantially equivalent to method claim 1. Therefore, claim 29 is rejected under a similar rationale.

Regarding Claim 2,

The method of Kephart et al. modified by Wells and Albrecht does not disclose the different security events that can occur when a virus is detected.

Wells, however, discloses that the security event is selected from a group consisting of cleaning the data (Column 9, lines 25-26), quarantining the data (Column 9, lines 39-41), and blocking the data (Column 9, lines 39-41). To quarantine a file is to block access to it and, optionally, send it to a special directory devoted to quarantined files, thus blocking the data is broader than quarantining the data. This new method would be the method of Kephart et al. modified by Wells and Albrecht allowing a certain security event to be chosen when the data is found to contain a virus.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use these different security events in order to obtain a more versatile virus detection system that can handle data in a proper manner. One of ordinary skill in the art would have been motivated to do so in order to be able to use a different function depending on what is wrong with the file.

Regarding Claim 16,

Claim 16 is a computer program product claim that is substantially equivalent to method claim 2. Therefore, claim 16 is rejected under a similar rationale.

Regarding Claim 3,

Kephart et al. disclose the step of reporting that the data is innocent, by way of original data being output if the data is successfully compared to the fingerprints of innocent data (Column 5, lines 33-36). It would only take 1 reconstruction to determine that the current file matches that of the fingerprint for that file.

Regarding Claim 17,

Claim 17 is a computer program product claim that is substantially equivalent to method claim 3. Therefore, claim 17 is rejected under a similar rationale.

Regarding Claim 4,

The method of Kephart et al. modified by Wells and Albrecht does not disclose that the information transmitted to the server includes the data.

Albrecht, however, discloses that the information transmitted to the server includes the data (Detailed Description, Paragraph 48). This new method would be the method of Kephart et al. modified by Wells and Albrecht sending all of the data as information to the server.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to send all of the data to the server because the virus detection utility may require all of the data in order to detect viruses. One of ordinary skill in the art would have been motivated to do so in order to provide adequate information to the server when it needs more than just a fingerprint of the data to be checked for viruses.

Regarding Claim 18,

Claim 18 is a computer program product claim that is substantially equivalent to method claim 4. Therefore, claim 18 is rejected under a similar rationale.

Regarding Claim 5,

The method of Kephart et al. modified by Wells and Albrecht does not disclose that the information transmitted to the server includes a fingerprint associated with the data.

Albrecht, however, discloses that the information transmitted to the server includes a fingerprint associated with the data (Detailed Description, Paragraphs 47 and 48). This new method would be the method of Kephart et al. modified by Wells and Albrecht sending a fingerprint of the data as information to the server.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to send only a portion of the data to the server in order to reduce the amount of data that must be sent to the server. One

of ordinary skill in the art would have been motivated to do so in order to reduce the amount of data that must be transferred between a client and a server for the purpose of virus detection (Summary, Paragraph 6).

Regarding Claim 19,

Claim 19 is a computer program product claim that is substantially equivalent to method claim 5. Therefore, claim 19 is rejected under a similar rationale.

Regarding Claim 6,

Kephart et al. disclose the step of comparing the fingerprint associated with the data and fingerprints associated with innocent data in a third database (Column 5, lines 2-13), but not that this database is at the server.

Albrecht discloses that the comparison is done with a database at the server (Detailed Description, Paragraph 48). This new method would be the method of Kephart et al. modified by Wells and Albrecht comparing the fingerprint associated with the data and fingerprints associated with innocent data at the server.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to compare the fingerprint associated with the data and innocent fingerprints in a database at the server in order to allow for fewer databases to be updated every time the innocent data must be updated. One of ordinary skill in the art would have been motivated to do

so in order to reduce the number of innocent data updates required, improving security of the network (Background, Paragraph 3).

Regarding Claim 20,

Claim 20 is a computer program product claim that is substantially equivalent to method claim 6. Therefore, claim 20 is rejected under a similar rationale.

Regarding Claim 7,

The method of Kephart et al. modified by Wells and Albrecht does not disclose comparing the fingerprint to virus definitions at the server.

Albrecht, however, discloses the step of comparing the fingerprint associated with the data and fingerprints associated with virus definitions in a fourth database at the server (Detailed Description, Paragraph 48). This new method would be the method of Kephart et al. modified by Wells and Albrecht comparing the fingerprint to virus definitions in the server.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to compare the fingerprint with virus definitions in order to ascertain whether there is a virus in the data on the client computer. One of ordinary skill in the art would have been motivated to do so in order to determine whether there is a virus on the client computer and perform the proper actions if so.

Regarding Claim 21,

Claim 21 is a computer program product claim that is substantially equivalent to method claim 7. Therefore, claim 21 is rejected under a similar rationale.

Regarding Claim 9,

The method of Kephart et al. modified by Wells and Albrecht does not disclose sending the entire data when the fingerprint isn't enough.

Albrecht, however, discloses transmitting the data to the server utilizing a network upon an unsuccessful comparison of the fingerprint associated with the data and fingerprints associated with the innocent data and virus definitions at the server (Detailed Description, Paragraph 48). This new method would be the method of Kephart et al. modified by Wells and Albrecht sending more data as the server needs it and sending all of the data in the case when the server needs all of the data to make a determination as to whether the data contains a virus.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to send more than just the fingerprint to the server in order to give the server enough information to determine whether the data contains a virus. One of ordinary skill in the art would have been motivated to do so in order to reduce the amount of data that must be transferred between a client and a server whenever possible, only sending the full data when it is absolutely necessary (Summary, Paragraph 6).

Regarding Claim 23,

Claim 23 is a computer program product claim that is substantially equivalent to method claim 9. Therefore, claim 23 is rejected under a similar rationale.

Regarding Claim 10,

The method of Kephart et al. modified by Wells and Albrecht does not disclose analyzing the data transmitted to the server.

Albrecht, however, discloses the step of analyzing the data transmitted to the server (Detailed Description, Paragraph 49). This new method would be the method of Kephart et al. modified by Wells and Albrecht analyzing the data that is transferred to the server when the fingerprint is found lacking.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to analyze the data transmitted to the server in order to attempt to clean the data. One of ordinary skill in the art would have been motivated to do so in order to try to clean the data before not allowing access to it.

Regarding Claim 24,

Claim 24 is a computer program product claim that is substantially equivalent to method claim 10. Therefore, claim 24 is rejected under a similar rationale.

Regarding Claim 11,

The method of Kephart et al. modified by Wells and Albrecht does disclose that the data is transmitted to the server in separate parts (Albrecht, Detailed Description, Paragraph 48).

Regarding Claim 12,

The method of Kephart et al. modified by Wells and Albrecht does not disclose updating a database based on the analysis.

Wells, however, discloses the step of updating at least one of the first database, the second database, the third database, and the fourth database based on the analysis (Column 10, lines 8-13). This new method would be the method of Kephart et al. modified by Wells and Albrecht updating the first database based on the analysis.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to update at least one database in order to keep the system up to date. One of ordinary skill in the art would have been motivated to do so in order to allow virus scanning with the new virus detection and repair information.

Regarding Claim 14,

The method of Kephart et al. modified by Wells and Albrecht discloses that the first database and the second database are both components of a client computer. It does not disclose that the client computer is coupled to the server via a network.

Albrecht discloses that the client computer is coupled to the server via a network (Detailed Description, Paragraph 42). This new method would be the method of Kephart et al. modified by Wells and Albrecht communicating over a network.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to communicate over a network in order to allow the server to obtain data from the client computer and perform virus scanning on it. One of ordinary skill in the art would have been motivated to do so in order to have a communications system in which the server and client computer can exchange data.

Regarding Claim 28,

Claim 28 is a computer program product claim that is substantially equivalent to method claim 14. Therefore, claim 28 is rejected under a similar rationale.

Regarding Claim 25,

The computer program product of Kephart et al. modified by Wells and Albrecht does disclose that the data is transmitted to the server in separate parts (Albrecht, Detailed Description, Paragraph 48).

Regarding Claim 26,

The method of Kephart et al. modified by Wells and Albrecht does not disclose updating a database based on the analysis.

Wells, however, discloses updating at least one of the first database, the second database, the third database, and the fourth database based on the analysis (Column 10, lines 8-13). This new method would be the method of Kephart et al. modified by Wells and Albrecht updating the first database based on the analysis.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to update at least one database in order to keep the system up to date. One of ordinary skill in the art would have been motivated to do so in order to allow virus scanning with the new virus detection and repair information.

Regarding Claim 30,

Kephart et al. disclose a client-based method for detecting viruses in software, comprising comparing the data with fingerprints of innocent data in a second database (Column 5, lines 2-13).

Kephart et al. do not disclose comparing this data against virus definitions or sending the data to a server.

Wells, however, discloses the steps of comparing data with a plurality of virus definitions in a first database (Column 9, lines 19-20) and executing a security event if the data is successfully compared with at least one of the virus definitions (Column 9, lines 25-26). This new method would be the method of Kephart et al. modified by Wells and

Albrecht comparing the data against signatures of known viruses in a virus database.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use this other form of virus detection in order to expand the viruses that are detected by the system. One of ordinary skill in the art would have been motivated to do so because Kephart et al. suggest the use of other virus scanning software in combination with his method (Kephart et al., Column 12, lines 55-57).

Wells does not disclose transmitting the data to a server.

Albrecht, however, discloses the step of transmitting information to a server for analysis purposes if the client machine cannot identify the data as being either virus or innocent (Detailed Description, Paragraph 47). Albrecht also discloses the step of reporting [Return Scan Result Message] that the data is innocent if the data does not contain a virus (Detailed Description, Paragraph 48). This new method would be the method of Kephart et al. modified by Wells and Albrecht sending information to a server for further analysis.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to send information to a server for analysis in order to allow for fewer databases to be updated every time there is a new virus. One of ordinary skill in the art would have been motivated to do so

in order to reduce the number of virus updates required, improving security of the network (Background, Paragraphs 2 and 3).

Regarding Claim 31,

Albrecht discloses the following server-based method for detecting viruses in software in paragraphs 48 and 49 of the detailed description:

Receiving a fingerprint associated with data from a client computer for analysis purposes upon the data being unsuccessfully compared to virus definitions and fingerprints of innocent data stored on the client computer;

Comparing the fingerprint associated with the data and fingerprints associated with virus definitions at the server;

Requesting the data from the client computer utilizing a network upon an unsuccessful comparison of the fingerprint associated with the data, and the fingerprints associated with the innocent data and the virus definitions at the server (the server will request more data until all of the data has been requested to be sent to the server);

Receiving the data transmitted from the client computer in response to the request; and

Analyzing the data transmitted from the client computer.

Albrecht does not disclose the use of innocent data or updating of the virus definitions or innocent fingerprints.

Kephart et al., however, discloses the step of comparing the fingerprint associated with the data and fingerprints associated with innocent data at a server (Column 5, lines 2-13). This new method would be the method of Albrecht with the additional step of comparing the fingerprint of the data with innocent data stored at the server.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to compare the fingerprint of the data with innocent data in order to determine, with 1 simple comparison, if the data has been modified by a virus. One of ordinary skill in the art would have been motivated to do so in order to quickly determine whether a certain file contains a virus by comparing it against the innocent data from that file, as opposed to comparing it against many different virus definitions.

Kephart et al. do not disclose the step of updating the virus definitions or innocent fingerprints.

Wells, however, discloses the step of updating at least one of the virus definitions and the fingerprints of innocent data based on the analysis (Column 10, lines 8-13). This new method would be the method of Albrecht modified by Kephart et al. with the additional step of updating the virus definitions based on the analysis.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to update at least one database in order to keep the system up to date. One of ordinary skill in the art would have

been motivated to do so in order to allow virus scanning with the new virus detection and repair information.

Regarding Claim 32,

Claim 32 is substantially equivalent to claim 31, except that claim 32 only compares the fingerprint of data with virus definitions at the server, as opposed to comparing it with innocent data as well. This makes claim 32 broader than claim 31, thus allowing claim 32 to be rejected under a similar rationale.

Regarding Claim 33,

Claim 33 is substantially equivalent to claim 31, except that claim 32 only compares the fingerprint of data with innocent data at the server, as opposed to comparing it with virus definitions as well. This makes claim 33 broader than claim 31, thus allowing claim 33 to be rejected under a similar rationale.

3. Claims 8, 13, 22, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kephart et al. (U.S. Patent 5,613,002) in view of Wells (U.S. Patent 6,338,141) and Albrecht (U.S. Patent Application Publication 2001 / 0,005,889), further in view of Hodges et al. (U.S. Patent 6,035,423).

Regarding Claim 8,

The method of Kephart et al. modified by Wells and Albrecht does not disclose that the server databases are updated more frequently than those on the client computer.

Hodges et al., however, disclose that the third and fourth databases are updated more frequently (Column 6, line 64 to Column 7, line 8) than the first and second databases (Column 7, lines 9-19). This new method would be the method of Kephart et al. modified by Wells and Albrecht updating the databases on the server more frequently than the databases on the client computer.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to update the databases at the server more frequently than those on the client computer in order to distribute the updates to client computers when the client computers are available to receive the updates. One of ordinary skill in the art would have been motivated to do so in order to allow client computers to access the server at their convenience and download the updated information when, and only when, they are available and wish to do so (Column 7, lines 20-27 and lines 57-60).

Regarding Claim 22,

Claim 22 is a computer program product claim that is substantially equivalent to method claim 8. Therefore, claim 22 is rejected under a similar rationale.

Regarding Claim 13,

The method of Kephart et al. modified by Wells and Albrecht does not disclose that the information is transmitted to the server via the Internet.

Hodges et al., however, disclose that the information is transmitted to the server via the Internet (Column 6, lines 46-51 and Column 7, lines 28-32). This new method would be the method of Kephart et al. modified by Wells and Albrecht communicating over the Internet.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention for the client computer to communicate with the server vie the Internet in order to obtain a server that a company can keep virus information on. One of ordinary skill in the art would have been motivated to do so in order to obtain a single server that an antivirus company can keep updated and to allow distribution over the Internet from that server (Column 6, lines 27-45).

Regarding Claim 27,

Claim 27 is a computer program product claim that is substantially equivalent to method claim 13. Therefore, claim 27 is rejected under a similar rationale.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER